TASK ORDER

GST0013AJ0081

Issued to:

Northrop Grumman
7575 Colshire Drive
McLean, Virginia 22102

Under Alliant# GS00Q09BGD0056

In support of

The Defense Manpower Data Center

Program Management Office,
Defense Travel System

issued by:

The Federal Systems Integration and Management Center (FEDSIM)
3100 F St NW
Washington DC 20405
FEDSIM Project Number DE00637

C.1 BACKGROUND

The Defense Travel System (DTS) is a paperless electronic web-based system that enables Department of Defense (DOD) employees to determine availability of, and book, transportation and lodging reservations, and receive reimbursement through their financial institutions for out-of-pocket expenses. It also creates required financial transactions to provide funding for travel, identifies any deviations from statutes and regulations governing DOD travel, and archives electronic versions of documents in accordance with regulatory and statutory requirements. The mandated system for DOD temporary duty travel, DTS currently handles more than 70% of all travel of this type.

DTS resides on the DOD Non-classified Internet Protocol Routing Network (NIPRNet) circuit. DOD travelers access DTS using a web browser on their computers. Access control and digital signature capability are enabled using DOD Public Key Infrastructure (PKI) certificates. DTS is a Mission Assurance Category II, Sensitive (MAC II) system, however it operates in accordance with Mission Assurance Category I, Mission Critical (MAC I) requirements (see C.5.4 TASK 4 – INFORMATION ASSURANCE (IA)/SECURITY).

DTS currently services over 3 million DOD personnel. The system processes over 350,000 authorizations (travel orders) and 350,000 vouchers (requests for reimbursement) per month; however the current system has a capacity to handle up to approximately 470,000 vouchers per month to meet potential growth. In addition, the data storage capacity as currently configured is sufficient to handle storage requirements projected through 2015.

Government program management responsibility is assigned to Program Management Office – Defense Travel System (PMO-DTS) under the Defense Manpower Data Center (DMDC) (J-62). The Defense Manpower Data Center Program Executive Officer (PEO) as well as the Component Acquisition Executive (CAE) and the Defense Chief Management Officer (DCMO) are the Milestone Decision Authority (MDA). The Defense Travel Management Office (DTMO) is a key stakeholder in DTS and is responsible for management of the DTS Travel Assistance Center (TAC), the "help desk" for DTS users. The TAC is contracted by the DTMO and not part of this solicitation.

The primary Defense Travel System business process flows are shown in the graphic below.
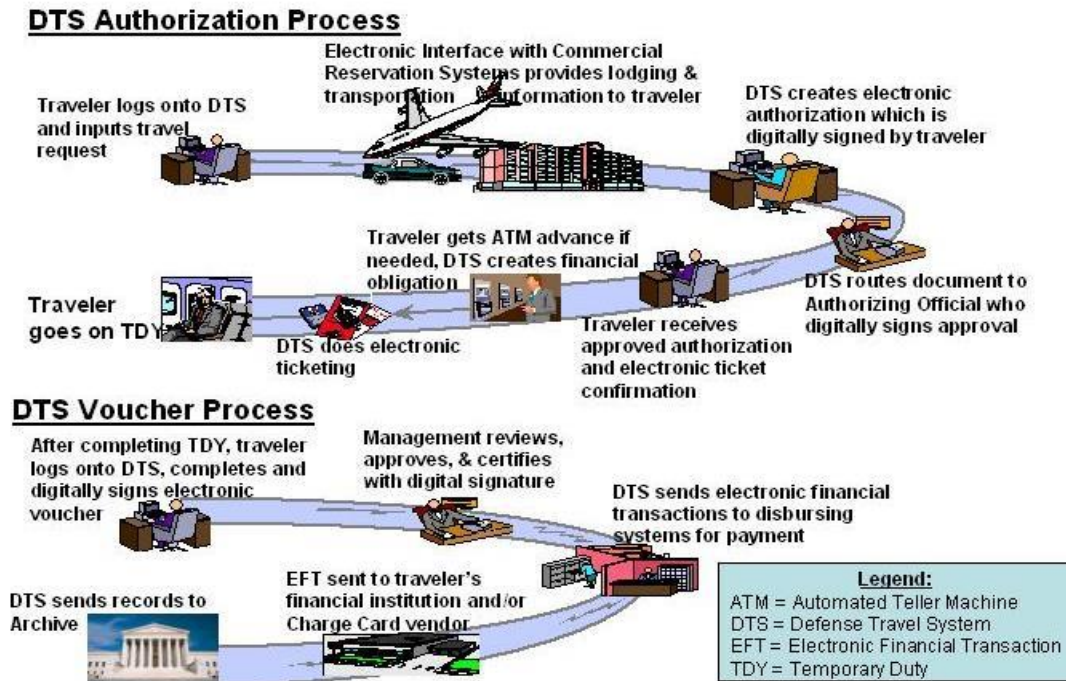
C.1.1 PURPOSE

The Government is awarding a Task Order to provide hosting, sustainment, and development of new capabilities for DTS.

C.1.2 AGENCY MISSION

DMDC Information Operations, Enterprise Solutions and data services organization is responsible for delivering logistics mission success - through IT solutions sustainment; IT service strategy, management, and delivery; and cyber operations, mission assurance, and continuous improvement. DMDC's strategy is to provide assured computing through systems, services, and partnerships that are operationally secure and efficiently managed, continuously evaluated for technology insertion and process improvement, and deliver best-in-class service.

C.2 SCOPE

The contractor shall provide the production environment to operate the system, including primary and backup facilities. This shall include, hosting the current DTS software, physical architecture design, providing all necessary computing networking, and telecommunication hardware, as well as all software required for operating systems, network operations and management, and any other commercial, non-application software needed to enable operation of DTS. The Government currently provides the hardware and information assets required, for hosting the system. The Government may move toward hosting as a service in the longer term but the Contractor during the term of this Task Order, but initially the Contractor shall be

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

required to use the hardware and software provided by the Government. The scope also includes the maintenance of the environment, identifying, trouble-shooting, and repairing problems, and ensuring DTS' availability to users in accordance with system performance requirements (see QASP).

System security is also a contractor responsibility, including physical protection of the facility, system certification and accreditation, and other related security requirements.

Sustainment provides for application software maintenance (the DTS application software will be provided as Government Furnished Equipment / Government Furnished Information (GFE/GFI)). This will include trouble-shooting and fixing defects as specified on System Problem Reports (SPRs); incorporating Change Requests (CRs) and, supporting the resolution of Help Desk tickets. Sustainment includes integrating the application software into the DTS environment, and designing and maintaining the logical architecture of the software and system.

The Contractor shall provide DTS development to include coding and functional testing of new capabilities in the application software. It may require framework architecture design and implementation along with database and data object design and development. It requires full adherence to an approved Systems Development Life Cycle (SDLC).

C.3   CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

The following sections provide a general description of the current DTS operating environment. Complete lists of software and hardware configuration items to be provided to the contractor as Government Furnished Equipment (GFE) and Government Furnished Information (GFI) are provided in the Technical Data Package.

C.3.1 Hardware

The DTS hardware environment currently includes commercially available information technology and telecommunications equipment operating in a three-tiered architecture: a web tier, an application tier, and a database tier. Two (2) production environments are in operation along with one (1) lab environment:

- Central Data Center (CDC) 1 (the primary site) is used to support production (normal system operation)
- CDC 2 (the secondary site) provides system backup; operates as the Continuity of Operations (COOP) site; and is also partitioned to provide environments for training Government users and for testing new application software.
- Lab environment is used for software remediation and development and testing of new software capabilities. This includes white box and integration testing of application software. The lab is currently located at the contractor facility.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

Production Hardware is currently located at data centers in the National Capital Region – CDC 1 in Sterling, VA and CDC 2 in Annapolis, MD. The hardware in these environments will be provided to the contractor as GFE.

In the event that CDC 1 is unable to operate normally, CDC 2 is used as a fail-over COOP site to continue support of users. The databases between these two (2) facilities are synchronized to prevent data loss. DTS has a requirement for a minimum of 98.5% operational availability (excluding Government-approved down time) of the primary site (measured 24x7x365 with maintenance periods limited to Government-approved downtimes), and a system performance requirement for an average web page response time of not more than two (2) seconds during any hourly increment of any day. When the primary site fails over to the COOP site, (CDC 1 to CDC 2) and, CDC 2 is operating as the primary production site; the test and training environments are no longer available and CDC 2 shall meet the same performance – operational characteristics and metrics as CDC 1. Details pertaining to Hardware environments can be found in Environment Section of the Technical Data Package (TDP) (Section J, Attachment J). This includes all necessary operating system software and tools required to operate the environment.

Current DTS GFE system can process up to 470,000 vouchers per month, and current DTS GFE data storage capacity is expected to be sufficient to cover DTS usage through 2015. However, DTS may grow in terms of additional application software functionalities, potentially requiring supplementary hosting system computing resources or data storage. The Government seeks to take advantage of new developments and efficiencies in hardware and software industries.

C.3.2 Software

The DTS application software was developed and maintained under contract to the Government. The DTS software is Government owned and will be furnished, along with associated documentation (such as requirements and design documents, version descriptions, and test specifications and results) to the contractor as GFI. Software and associated information assets provided as GFI are listed in the TDP. The Government will furnish DTS application software along with all other DTS information assets, as it exists at the time of task order award to the contractor. Supporting documentation will be furnished as part of the TDP and as part of the transition plan documents required of the Incumbent contractor. Certain items such as network management tools, performance monitoring tools, etc. shall be procured and maintained by the contractor.

C.3.3 Network and Interfaces

The following network and system interfaces are currently in operation within DTS:

- DTS web portal for user access to the system
- Connection with Defense Information Systems Agency (DISA) NIPRNet
- Interfaces via NIPRNet with:

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

- o DISA PKI for download of daily Certificate Revocation List (CRL) used for user access verification
- o Defense Manpower Data Center (DMDC) Archive/Management Information System for archiving of electronic travel records
- o DISA Global Exchange Service (GEX) to interface with DOD financial systems

- Interfaces via commercial networks or dedicated lines with:

  - o Government Travel Charge Card Vendor (GTCCV)
  - o Global Distribution Systems (GDS), Commercial Travel Offices (CTOs) and Travel Service Providers via OpenJaw for information on and reservations for travel arrangements
  - o ITA Software for commercial airline reservation information.

C.3.4 Three Tier Helpdesk Model

The DTS helpdesk employs a three-tier standard industry model for servicing DTS user problems. Oversight for the first two (2) tiers is managed by the DTMO and is not a requirement for this Task Order. A list of DTMO points of contact (POCs) will be provided upon award to ensure currency. Oversight for the third tier is managed by PMO-DTS and is a requirement for this Task Order. Tier roles are as follows:

Tier 1 (T1HD), is the first line user-facing support, and responsible for analyzing/classifying user problems, initiating help desk tickets and solving simple technical and user issues. The goal for this group is to solve 80% of all user problems and 50% of all technical problems.

Tier 2 (T2HD) consists of technical and business specialists who address more complex issues. They apply advanced technical or administrative support troubleshooting and analysis techniques. The T2HD goal is resolve 95% of remaining user related problems and 80% of remaining Technical related problems. The T2HD group will validate and prioritize technical problems before elevating them to the Tier 3 group.

Tier 3 (T3HD) support is the responsibility of the Contractor. T3HD staff is required to resolve all remaining detailed technical issues. Examples of these issues include coding defects; database or data object problems and system or hardware failures. These are expected to be technical issues that require examination and correction of code or data that is not otherwise accessible to T1HDs or T2HD. The process by which issues are currently escalated to the T3HD includes the capturing of the users work process when encountering the issue (via screenshots), a description of the problem, and an impact statement on behalf of the user. This information is compiled into a Software Problem Report (SPR).

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

These technical issues and their resolution will be assigned an SPR priority as defined below.

C.3.5 SPR Priorities

SPRs are categorized into the following priority levels and disposition is determined by the Governance Body. See Section J Attachment H, Additional Agency Guidance for a summary of current SPRs by priority. The Governance body consists of the made up of ad hoc members, as necessary, and may include the functional sponsor, user representatives, program office personnel and the contractor.

- o   Priority 1 (P1) - CRITICAL - Any problem that will prevent the system from being deployed, or, once deployed, will cause the system to be unavailable, or prevents the accomplishment of a mission-essential capability.
- o   Priority 2 (P2) - SERIOUS - Any system problem that adversely affects or prevents a user from executing a mission-essential capability for which there is no acceptable workaround.
- o   Priority 3 (P3) - MODERATE - Any system problem that prevents a user from executing a mission-essential capability, but has a **government approved,** acceptable workaround.
- o   Priority 4 (P4) - MINOR - Any system problem that presents operator inconvenience but does not affect the accomplishment of a mission-essential capability.
- o   Priority 5 (P5) - COSMETIC - Any system problem or change that is merely cosmetic (typographical errors that do not change the meaning of an instruction or a message, a more descriptive error message, etc.).

C.4   OBJECTIVE

The principal objectives of this Task Order are stated below:

The contractor shall use existing DTS system GFE hardware and GFI operating system software for initial hosting of DTS. Note: This current GFE system has demonstrated the ability to meet the contract performance requirements specified in the QASP. Within the life of the Task Order, the Government intends to migrate from a Government-owned hosting environment to a Contractor Furnished Equipment (CFE) environment where hosting is provided as a service.

The contractor shall manage and maintain two (2) CDCs: CDC 1 (production environment) to operate the system; and CDC 2 (physically separate backup facility) for Disaster Recovery (DR), Continuity of Operations (COOP), load and performance testing, and end user training. Note: Physical facilities for housing CDCs must be located in the contiguous continental United States. Equipment connected to the circuits shall be installed, tested, and successfully complete a DOD Information Assurance Certification and Accreditation Process (DIACAP) accreditation, obtaining either an Authority to Operate (ATO) or an Interim Authority to Operate (IATO).

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

The contractor shall provide sustainment support to include maintaining the existing DTS functionality, software defect remediation, maintenance of DTS interfaces, operational support to ensure that the DTS application is available on a 24x7x365 basis, and T3HD support.

The contractor shall provide potential new development to include enhancements to existing DTS functionality. This may include enhancements to ensure compliance with new regulations, user requests, new interfaces, and adaptation to changes in the commercial travel market.

C.5   TASKS
C.5.1 TASK 1 – HOSTING SERVICES

C.5.1.1 SUBTASK 1.1 – Hosting Migration Planning for GFE

The Contractor shall provide a Hosting Migration Plan (Preliminary and Final) in accordance with Section F.5, for the physical movement of both CDCs to contractor's sites. The plan shall reflect a series of specific test events with measurable and verifiable success criteria identified for each step, to ensure DTS transition is fully operational and ready to service DTS user community web traffic. Government requires transition to be fully completed (i.e., both CDCs moved and fully operational) as early as practicable, but not later than three (3) months after NIPRNet connectivity is established.

The Hosting Migration Plan must address, at a minimum, the areas below and incorporate the process and sequence details for moving COOP and PROD sites:

a. Migration activities with third party equipment vendors as required to successfully complete the installation of the DTS equipment.
b. Migration activities during periods of low user activity such as weekends with the site being unavailable for more no more than 72 hours.
c. Facilities preparation, power, fire suppression, security, environmental, space plan, cabling/wiring, rack layout etc.
d. Physical server and network architecture that is fault tolerant
e. Inventory control of the GFE
f. Installation details of Servers for the Web and Application Tier with High Availability/failover & system redundancy details
g. Installation details of Data Tier Server, primary storage disc arrays, secondary storage, PRI server and peripherals
h. Network Installation to include: NIPRNet circuits and related hardware, site-to-site communications, T1 / facsimile lines, VPN equipment, firewalls, and switches. Include test/validation time for these circuits/devices.
i. Installation and testing of all required Interfaces
j. Internet/DNS Registry & Protocol Management
k. Risk identification and mitigation planning for each step of the process using the Contractors Risk Management process.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

l. Management and oversight responsibilities with contact details
m. Milestones and critical success factors with demonstrable criteria
n. A separate test plan for each move (CDC 1, CDC 2 and an integrated test for the full operational profile)
o. Cut over plan for each move and a final cut over plan with acceptance criteria for full operational mode
p. A detailed list of all substituted components, if any, and a recovery statement that includes a secure location, point of contact, and scheduled times the Government can recover the unused GFE components.
q. The process and sequence details for moving COOP and Production (PROD) sites.

A complete, detailed GFE listing is located in the TDP. GFE will include, but is not limited to web servers, application servers, database servers, routers, load balancers or other network components. GFI will include, but is not limited to, operating systems, software tools, utilities and other software to operate system hardware.

The Government will maintain responsibility for funding and contracting for any required physical relocation of GFE from current locations to new hosting sites. The PMO representative will initiate processes for installing NIPRNet connectivity to new CDC sites. It is estimated the process may take up to three (3) months to establish these connections. To mitigate risk, the CDC 2 site shall be initially moved, followed by the CDC 1 site. Once NIPRNET connectivity is complete, the first set of GFE will be moved from CDC 2 to the contractor backup site; Contractor shall accept GFE and manage installation in their facility. Incumbent Contractor shall be available to provide any technical support for transfer and installation as required. The follow-on contractor must conduct and obtain full DOD IA security accreditation at the new sites; this process may take up to sixty (60) days before the site is certified and ready to "go live." After the first site goes live, GFE move process will be repeated for moving CDC 1 hardware to the follow-on contractor's second site.

The conceptual plan is for contractor to disable the database synchronization, the primary storage disc arrays and power down CDC 2. The PMO will oversee system transfer to the follow-on contractor's backup site, and the Contractor shall install, test, then power up CDC 2, sync the transactional data/disc arrays and cutover system production to CDC 2. Moving, testing and syncing for CDC 1 follows, with production operations switching back to CDC 1 and backup environment restored in CDC 2. A maximum of seventy-two (72) hours of continuous non-availability is allowed during the final reconfiguration for CDC 1 (production) and CDC 2 (COOP).

Government will provide line connections to NIPRNet for new sites as required within ninety (90) days of award. Installation of NIPRNet circuits requires that Hosting services include designing physical architecture of system and networks; providing all necessary computer networking and telecommunication hardware not supplied as GFE; providing all software not supplied as GFI required for operating systems, network operations and management; providing any other commercial, non-application software needed to enable operation of DTS; and

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

maintaining all hardware support service agreements and all software licensing agreements for DTS. Hosting services include performing System Administrator functions; identifying, trouble-shooting, and repairing problems; and ensuring DTS availability to users in accordance with system performance requirements. Hosting services include providing physical protection of facilities, supporting the Government with system certification and accreditation activities, and other related system security and Information Assurance (IA) requirements. Hosting services also include system backup activities and Information Technology (IT) Contingency Planning, including coordinating with PMO-DTS to schedule exercises for system fail-over to the CDC 2 facility.

C.5.1.2 SUBTASK 1.2 – Hosting Transition Planning for CFE (Optional CLIN X005)

DTS may experience future growth in terms of additional application software functionalities requiring supplementary hosting system computing resources or data storage. The contractor shall take advantage of new developments and efficiencies available in the hardware and software industries that could accommodate such growth through the normal hardware technical refresh process or improved efficiencies in the application software or software frameworks.

Upon approval of the CO, and upon the exercise of the option GFE to CFE Transition Planning CLIN, the contractor shall provide a GFE to CFE Transition Plan, in accordance with Section F.5, for migrating DTS hosting to a fully CFE environment. The plan shall include demonstrable milestones and associated metrics for success factors that the Government must evaluate and approve prior to transitioning to CFE shall that will ensure compatibility with DTS application software and all other information assets.

At a minimum, the GFE to CFE Transition Plan shall address:

a. Transition to CFE during period of low user activity such as weekend with site being unavailable for no more than 72 hours..

b. The overall strategy for accomplishing the migration. Contractor shall address the resources required, identify the transition team's organization and responsibilities, as well as the tools, techniques, and methodologies that will be used to perform an efficient and effective transition.

c. A project schedule, resource estimates and identification of special requirements.

d. The transition plan shall also define management controls and reporting procedures, as well as the risks, risk mitigation and contingency plans that will eliminate operational failure including roll-back to the GFE production environment. A statement outlining the potential impact of the transition to the CFE infrastructure in terms of ongoing software development and database changes must be included.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

e. Milestones, critical success factors and a final test plan for verification of a successful migration in terms of operational software and production data.

f. A decommissioning section for the GFE that includes full inventory control shall be included and comply with DoD regulations for all such activities.

g. Application Migration:

- Design architecture for CFE sites (Web/App/Data/Storage)
- Setup and configure frameworks
- Perform configuration control and validate architecture
- Install software, validate to acceptance criteria
- Migration of production and support data against Contractor's data migration assurance test plan
- Testing for zero transactional data loss and recovery
- Integration and data integrity testing and mitigation of problems
- User acceptance testing and sign off procedures
- Comparison of CFE environment to GFE environment (functional, response time and loaded response time)
- Final documentation process

h. Operation Testing:

- Soft launch the system and operate under load
- Monitor performance and identify anomalies
- Produce configuration controlled operations log
- Conduct reviews of operations logs with Government

i. Provide an addendum(s) with test plans associated with tasks that require testing.

j. Internet/DNS Registry & Protocol Management

k. Status of Contractor Furnished Equipment (CFE) relative to approval by the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS).

l. Hardware Equipment List for submittal to the Government for review/approval prior to transition to CFE Hosting

m. Network Preparation Plan/Schedule for CFE Hosting

n. Network Installation Plan/Schedule for CFE Hosting

o. DTS System Verification Test Plan for CFE Hosting

p. Plan for DIACAP certification & accreditation.

The transition, if exercised, shall be completed within 12 months after contract authorization to proceed.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

Upon completion of the transition from the GFE to the CFE environment, and after PMO and the COR acceptance, the run book requirement in **Hosting Transition Planning for GFE** is not required.

C.5.1.3 SUBTASK 1.3 – Hosting Transition Out Planning

The Contractor shall provide a Hosting Transition-Out Plan, in accordance with Section F.5, to transition DTS application Hosting services. The transition may be to a follow-on contractor or a Government entity and must reflect either a GFE or a CFE environment, whichever is in effect at the time the plan is requested. It is anticipated that the Hosting Transition-Out would occur at the end of Option Year Four (4) (should all four options be exercised), with a period of performance not to exceed nine (9) months to complete final transition.

Significant knowledge transfer will likely be required to complete a seamless transition to a new Hosting entity. The Contractor's plans must reflect an approach that transfers required knowledge without divulging any proprietary information, and ensures a successful transition, with no more than seventy-two (72) hours of production downtime before establishing full operational capability at the new hosting facility.

Detailed requirements and time required to execute Transition-Out may vary depending on the Contractor's operational concepts and specifics of CFE –vs- GFE hosting environments at the time of transition.

Four (4) months prior to transition, the contractor shall provide a transition plan for CDC 1 and CDC 2 migration to a new contractor with all the activities and tasks required to maintain and sustain all the hardware and related operating systems software for both CDCs.

C.5.1.4 SUBTASK 1.4 – Operational Hosting Services

The contractor shall perform the following specific tasks:

- Maintain the computing environment to achieve and sustain performance and availability requirements as stated in the following sections: **Operational Availability Requirement** and **System Performance Requirements** and **Performance Tuning**.
- Manage network connections to the established end points of demarcation. As per common business practices, hosting services involve layers 1, 2, 3 and 4 of the Open Systems Interconnection Model used by industry. (The sustainment and development services involve layers 5, 6 and 7.).
- Manage and maintain the operating system software and the general operating environment.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

- Manage and maintain all third party software including patches and upgrades from the appropriate vendors. Manage upgrade activities and third party license issues as they pertain to the system environment.
- Perform the duties as Oracle Database Administrator (DBA) for the database (DB) server administration and data synchronization.
- Perform any other action in accordance with standard practices and operating procedures to maintain system performance and availability requirements.
- Monitor system performance testing and final stage functional testing on the backup site to assure newly developed code, data structures and frameworks comply with performance specifications before release to the production system.
- Manage, plan, advise, and implement system capacity, scaling, and obsolescence details and activities, including system component end-of-life issues.
- Collect and review operational and system performance metrics as required ensuring service delivery requirements are met, see QASP.
- Prepare and implement (if CO-exercises CFE Transition option) a plan to decommission GFE environment.
- Maintain, modify, update, and submit DTS documentation. Documentation will be submitted in electronic format.

Decisions on operational issues, all non-availability periods, software migrations, release schedules, system upgrade and changes, and any related risks assumed by the Government will be made by the PMO. As directed by the Program Manager for the DTS effort, designated personnel that support the DTS, shall have access to the contractor facilities. In no case shall contractor deny the Government access to inspect contractor's facilities. This includes the production environment (CDC 1 and CDC 2) and the testing and lab environment.

Government requires multiple data points/metrics provided at varying intervals in order to ensure effective program management of the DTS. These data points/metrics consist of real-time, regularly scheduled, and ad hoc DTS performance information. The Contractor shall provide additional operational metrics, as required and consistent with standard industry practices, to the Government.

C.5.1.4.1 Operational Availability Requirements

The DTS system operational availability shall be a minimum of 98.5%, measured 24x7x365 with maintenance periods limited to Government approved downtimes. Documentation of system operational availability shall be reported on a periodic basis. Operational availability requirements apply to both Production and COOP systems. Downtime approvals are issued by the Government for routine and emergency maintenance of the system and its physical and logical components, upgrades to the software or hardware components of the system, and for testing, when such testing requires making DTS unavailable to the users. The Contractors shall provide a rationale and schedule for all downtime events and the Government must approve in

advance. Approved downtime that complies with the advanced Government approval shall not affect the Contractors performance metrics.

C.5.1.4.2 System Performance Requirements

System performance requirement is an average web page response time of not more than two (2) seconds during any hourly increment of any day for the production system. This will be measured inside the DTS firewall and assessed on a monthly basis (based on calendar days). Documentation of system performance shall be incorporated into the Monthly Status Report.

C.5.1.5 SUBTASK 1.5 – Performance Tuning

The contractor shall be responsible for monitoring the performance of all physical and logical components of the system. This shall include all operational metrics such as Central Processing Unit (CPU) and memory consumption, network bandwidth and server request/reply response times, plus any other usual and customary system parameters as is normal in commercial best practices for the contractor's hosting operations. The Contractor shall use ISO 9001:2008. The contractor shall tune or adjust the system components to meet the minimum system requirements.

C.5.1.6 SUBTASK 1.6 – System Backup

All data, software operating environments, plus configurations for those environment(s) and machine readable application code shall be fully backed up after any incremental change. Contractor shall also provide any other electronic files, software, or other items necessary to restore environments to an operational status. In addition, whenever the contractor changes configuration of hardware, architecture or other contractor-owned or leased software, contractor shall deliver these changes via electronic means, within one (1) week of making such change.

Backups shall be delivered within one (1) week. These shall be machine-readable electronic media to be proposed by the contractor, or using file transfer methodologies. The government will verify delivery of the backups to the approved facility through review of security logs. The Contractor shall not rely upon these backups for their operations.

C.5.1.7 SUBTASK 1.7 – Configuration Management

Configuration management includes all standard system software to facilitate System Administrator and management roles. Configuration Status Accounting Information shall be tracked and reported in the Configuration Item Identification Inventory.

The Contractor shall procure Bill of Materials (BOM) items (see TDP for list of current BOM items). PMO DTS will seek approval of any new hardware items by the Designated Approval

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

Authority (DAA) to ensure National Information Assurance Partnership (NIAP) compliance. Once approved hardware is integrated into the DTS, the Contractor shall submit an updated network diagram reflecting the change.

The Contractor shall be responsible for maintaining all licensing, hardware support, and related agreements for all GFI and GFE. The Contractor shall ensure GFE is upgraded and/or replaced in accordance with the Government approved Configuration Management Plan. The Contractor shall not make substitutions for hardware or software that are not in accordance with the Government approved Configuration Management Plan.

C.5.1.7.1 Configuration Audit

The Contractor shall deliver the Configuration Audit Plan (CAP), in accordance with Section F.5, containing information required for conducting Functional Configuration Audits and Physical Configuration Audits. Use of MIL-STD-973 and MIL-HDBK-61A for guidance is encouraged:

The Contractor shall state the purpose and objectives of the audit in terms of the contract requirement for the audit. The following items shall be addressed in the CAP:

a. Identify the Hardware Configuration Items (HWCIs) to be audited. Each HWCI shall be identified by nomenclature, serial number, and any other applicable identifiers.

b. Identify the Computer Software Configuration Items (CSCI) to be audited. Each CSCI shall be identified by software title, code identification number, software inventory numbering system, and/or filename, as appropriate.

c. Summary of the hardware and software contractual requirements against which the audit will be conducted as specified in work statements, specifications and approved plans.

d. Outline of the proposed audit procedure for each item to be audited.

The Contractor shall identify proposed milestones for the audit(s). The Contractor shall provide the results of each audit to the Government, upon request.

C.5.1.8 SUBTASK 1.8 – Rollback Plan

The Contractor shall create, within thirty (30) days of completing transition of DTS to the contractor's CDC sites, a Rollback Plan – Operational Status for restoring DTS when any infrastructure modifications; operating system changes/patches; utility updates; configuration changes; or when any modifications to operating software for server or network components causes system failure, instability or a diminution of performance.

The Contractor shall create a Rollback Plan –Application/Configuration Changes for backing out application changes to software, frameworks and logical configurations within three (3) months of task order award.

The contractor may suggest a roll back to a previous version, or recommend not fielding a patch, release, or software change should they be able to show a negative impact to the DTS system's required performance criteria. The Rollback Plans can be incorporated into other documents, such as the Configuration Management Plan, or developed as internal technical documents that will be provided upon Government request.

C.5.2 TASK 2 – SUSTAINMENT AND DEVELOPMENT (S/D) SERVICES

C.5.2.1 SUBTASK 2.1 – Sustainment and Development Task Overview

The contractor shall perform the following specific tasks:

a. Provide program management associated with planning, monitoring, controlling, program execution, and lead integration.
b. Collect and analyze database statistics, events, availability, performance and trends.
c. Perform Configuration Management audits and identify configuration items throughout the SDLC process.
d. Provide the Government unrestricted access to the contractor's DTS technical and operational documentation via electronic means.
e. Attend meetings (such as Staff Meetings, Configuration Control Board, Program Reviews) as required by the COR.
f. Maintain and support a code vault and versioning system per industry best practices.
g. Maintain, modify and update DTS documentation. Deliver required in electronic format.
h. Deleted.
i. The Contractor shall provide any operational data to the Government upon request.

The required documentation deliverables are as follows:

a. Updates: minor modifications to the system aligned with the production baseline.
b. Deltas: significant modifications to the system, new documentation shall contain details describing only the changes, and shall align to the new production baseline.
c. Baselines: a full documentation package is created that includes all previous deltas and new changes. Baselines may be required at the request of the Government.

The Contractor shall create, maintain and update a DTS Operations Plan, in accordance with section F.5. The Operations Plan shall describe how the operational posture of DTS is managed and controlled. At a minimum, the plan shall include facilities, infrastructure (hardware,

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

operating systems), database management, DTS application monitoring/management, personnel, roles/responsibilities, and change management. The plan should also address:

    a.   What is required to run operations out of either CDC facility
    b.   Availability
    c.   Responsiveness
    d.   Hours of support
    e.   Scaling and Obsolescence process
    f.   Tools used

The Contractor shall receive the set of existing baseline documentation after Task Order award.

C.5.2.2 SUBTASK 2.2 – Engineering Changes

Engineering Change Proposals (ECPs) shall be provided in response to Functional Requirements Document (FRD) and Change Proposals (CP), or equivalent, submitted by the authorized PMO-DTS representative for enhanced, modified or new software capabilities. ECPs shall be provided in accordance with Section F.5.

The ECPs shall provide a sufficient description of the proposed change so that the Government CCB can make an informed decision on whether or not to proceed with the change, to include: background, description, requirements statements, VCRI statements, diagram visual process description, staffing/schedule estimates, and risk assessments (technical, schedule, and cost). Project summary shall be organized to include:

    a.   Work Breakdown Structure (WBS) Elements with rough order of magnitude (ROM) in hours

    b.   Schedule estimates for the project and impact (if any) on existing projects

    c.   Staffing requirements by roles and hours

    d.   Cost

    e.   Risk assessment for the project in terms of technical, schedule and cost

Once an ECP is approved by the government to proceed, then all drawings and diagrams, required for the various technical documents, impacted by the ECP shall adhere to the Department of Defense architectural Framework (DODAF) standards and delivered at PRR. Existing DODAF drawings and diagrams that are used shall be updated to the latest version. The DODAF designations herein refer to views in Version 2.0 (or most current version as of the date of solicitation.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

C.5.2.3 SUBTASK 2.3 – Interface Engineering and Development

The following section provides guidance on technical documents that are required to maintain accurate documentation of the DTS application and infrastructure.

Interface Requirements Specification:

For every interface development effort pursuant to an FRD (or equivalent), the Contractor shall deliver an Interface Requirements Specification (IRS). The IRS specifies the requirements imposed on one or more systems, subsystems, HWCIs, CSCIs, manual operations, or other system components to achieve one or more interfaces among these entities. The IRS shall be delivered within 30 days of a Production Readiness Review (PRR) milestone for new development activities. See DoD Data Item Description (DID) DI-IPSC-81434A for further guidance.

Interface Design Description:

The Contractor is responsible for maintaining existing interfaces, modifying existing interfaces and developing new interfaces (and related documentation) for the DTS. The government provides oversight and review of the results of the contractor's efforts through the PMO DTS test group. The Contractor shall provide an Interface Design Description (IDD) after completing any interface development or modification. The IDD describes the interface characteristics of one or more systems, subsystems, HWCIs, CSCIs, manual operations, or other system components. The IDD shall be delivered within 30 days of a PRR milestone for new development activities. See DoD DID DI-IPSC-81436A for further guidance.

C.5.2.4 SUBTASK 2.4 – Engineering Documentation for DTS Information Assets

The following section provides guidance on technical documents that are required to maintain accurate documentation of the DTS application and infrastructure.
Software Product Specification:

The contractor shall submit the revised Software Production Specification (SPS) for releases with new development or major content changes. An updated SPS is required at the production readiness review. An updated SPS is not required for a Sustainment release.

In documents where duplicate information exists, the contractor shall identify what document contains the required information and incorporate the information in other documents by reference. The referenced document shall reflect the most current production baseline.

The SPS contains or references the executable software, source files, and software support information, including "as built" design information and compilation, build, and modification

procedures for a CSCI. The SPS shall be delivered within 30 days of a PRR milestone for new development activities. See DoD DID DI-IPSC-81441A for further guidance.

System/Subsystem Specification:

For each new software release, (excluding SPRs) the Contractor shall deliver a System Subsystem Specification (SSS), to keep the SSS current with the current production baseline.

The SSS shall include flow control diagrams for internal system and provide traceability between the Configuration Items and the DTS System Requirements, including traceability of DTS System Requirements to Defense Travel Policy and Business Rules. The SSS shall comply with all requirements in IEEE/EIA 12207.1-1997 Lifecycle Data subsection: 6.26 System Requirements Specification.

If any of the information listed above is found in other documentation required by the PWS, that requirement shall be incorporated by reference to the other document providing the referenced document is up to date, per the current production baseline.

The SSS specifies the requirements for a system or subsystems and the methods to be used to ensure that each requirement has been met. The SSS shall be delivered within 30 days of a PRR milestone for new development activities. See DoD DID DI-IPSC-81431A for further guidance.

System/Subsystem Design Description:

The contractor shall provide a System/Subsystem Design Description (SSDD), describing the overall system and subsystem architectures needed to implement the DTS functional capabilities. It shall include system and subsystem component level architecture with sub and external system interface specifications using deployment diagrams, collaboration diagrams and sequence diagrams as required to accurately depict the architecture.

The SSDD shall comply with the requirements in IEEE/EIA 12207.1-1997 Lifecycle Data; subsections: 6.25 System Architecture and Requirements Allocation Description; 6.3 Concept of Operations Description.

The SSDD shall be delivered within 30 days of a PRR milestone for new development activities. See DoD DID DI-IPSC-81432A for further guidance.

Database Design Description:

The Contractor shall provide a Database Design Description (DBDD), in accordance with the requirements in IEEE/EIA 12207.1-1997 Life cycle Data, subsections: 6.4 Database Design Description. In the event requirements conflict with this PWS the PWS shall prevail.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

The DBDD describes the design of a database, that is, a collection of related data stored in one or more computerized files in a manner that can be accessed by users or computer programs via database management system (DBMS). The DBDD shall be delivered within 30 days of a PRR milestone for new development activities. See DoD DID DI-IPSC-81437A for further guidance.

Release Notes

For each software release (including SPRs) the Contractor shall deliver Release Notes detailing the contents of the release. This documentation shall be a supplement to the above documents and should detail the functional changes impacting the user community. Associated technical changes that may impact the user community shall be included as well. A draft of these release notes shall be available to PMO for review at the start of testing and shall be finalized prior to implementing the release in production. The Release Notes shall be available to the user community when the release is implemented and will be distributed through DTMO/TAC existing channels.

The Release Notes shall be labeled by both the common release name as well as the designated number for the release and a mapping of release name to number shall be maintained by the contractor. A repository of the Release Notes shall be maintained for future reference by PMO DTS. Release Notes are instrumental to future Government test, evaluation and audit activities.

C.5.2.5 SUBTASK 2.5 – Sustainment Services

The Contractor shall provide the following sustainment services:

- Maintain existing application software, middleware, frameworks, database, data objects, and perform ongoing defect remediation and updates.
- Support planning and control of all system operations, capacity planning and maintenance activities.
- Implement routine maintenance and installation of software and middleware products.
- Monitor and support DTS databases data and objects and any applications of middleware associated with them.
- Trouble-shoot and resolve data issues.
- Maintain logical component of system interfaces.
- Provide, maintain, operate and support a software defect tracking tool, and provide PMO electronic access for at least fifteen (15) concurrent users. The tool shall, at a minimum, have the capability to include the following information about software defects, including SPRs: tracking number, title, description, priority, functional area, user impact, and proposed release to incorporate repair. The tool shall support the migration of existing remediation information.

- Maintain and manage software and updates for GDS, OpenJaw, ITA software and all other logic components of the system, including detailed analysis of logs and system configurations and remediation of problem issues associated with such components.
- Perform tasks required to achieve system stability of operation for both CDC 1 (production) and CDC 2 (COOP) systems (such as routine recycling of application and middleware components as required).
- Support for software, interfaces and other logical components of the system to ensure transactional and archival integrity of all financial data and interface information.
- Maintain a development and lab environment(s) to support source code and logic component remediation. Such environment(s) shall include ability to test new code fixes, configuration modifications and updates or modifications to any logic components of the system. The environment shall allow for full integration testing in accordance with industry best practices. Environment(s) must include ability to test against a representative data set, simulate transactions and interface stubs as required.

The contractor shall provide dedicated workspace (hotelling cubicles with telephone and direct high speed internet) at the sustainment/development site for concurrent use by up to five PMO DTS government staff.

C.5.2.6 SUBTASK 2.6 – Development Services (Optional CLIN X004)

The contractor shall perform the following tasks:

- Design and implementation of CRs for enhanced software functionality or improved usability.
- Deleted
- Analyze system engineering and architectural issues, lead efforts in planning, analysis, engineering review, improvement and integration of DTS architecture as relates to all software servers, frameworks, application software, middleware, and databases.
- Develop logical components for system interfaces.
- Provide, maintain, operate and support a requirements versioning tool, and provide the Government electronic access for at least fifteen (15) concurrent users. The tool shall, at a minimum, have the capability to migrate existing software requirements and their respective versions.
- Provide, maintain, and operate environments for software development and contractor and Government testing.
- Maintain development and lab environment(s) to support source code development or newly acquired software products. Such environment(s) shall include ability to test newly developed code up to and including full integration testing in accordance with industry best practices. Environment(s) must include ability to test against a representative data set, simulate transactions and interface stubs as required. Government access for integration and initial functional tests shall be provided.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

- Support the creation of external connections to the reporting database. The Contractor shall maintain and provide updates to the users' guide (at a minimum bi-annually) if development efforts , changes modifications, or expanded tool functionality/capability warrants.
- Support the development of additional reports and associated data elements to the data mart based upon new reporting requirements.

The Contractor shall provide a Software Development Plan (SDP) in accordance with Section F.5. The SDP describes a developer's plans for conducting a software development effort, including the SDLC and related milestones, while minimizing risk.

The plan shall contain all requirements in "IEEE/EIA 12207.1-1997 Life cycle Data" subsections: 6.5 Development Process Plan, 6.11 Project Management Plan, 6.17 Software Development Standards Description and 6.18 Software Integration Plan. See DoD DID DI-IPSC-81427A for further guidance.

The contractor shall provide a Software Version Description (SVD) for each version of production software at the PRR milestone. The SVD identifies and describes a software version consisting of one or more CSCIs. It is used to release, track, and control software versions. The SVD shall comply with all requirements in IEEE/EIA 12207.1-1997 Lifecycle Data" subsections: 6.13 Software Configuration Index Record. Develop enhanced or new capabilities for application software, middleware, frameworks, database, and data objects. See DoD DID DI-IPSC-81442A for further guidance.

The Contractor shall also submit a Software Design Description (SDD). The SDD describes the design of a CSCI. The SDD shall include the requirements in "IEEE/EIA 12207.1-1997 subsections: 6.12 Software Architecture Description, 6.13 Software Configuration Index Record and 6.16 Software Design Description. The SDD shall be delivered within 30 days of a PRR milestone for new development activities. See DoD DID DI-IPSC-81435A for further guidance.

For newly developed software the Contractor shall provide a Software Requirements Specification (SRS). The SRS specifies the requirements for a CSCI and the methods to be used to ensure that each requirement has been met. The SRS shall adhere to the requirements in "IEEE/EIA 12207.1-1997 Life Cycle Data" subsections: 6.22 Software Requirements Description and 6.27 Test or Validation Plan. The SRS shall be delivered within 30 days of a PRR milestone for new development activities. See DoD DID DI-IPSC-81433A for further guidance.

Development services include implementing new capabilities as defined in a Government-provided Functional Requirements Document (FRD), or equivalent, when issues by a Government POC. Software engineering studies and analyses, design and development of new software and framework architectures, middleware, interfaces, and interface protocols, as well as modifications to existing interface protocols, may also be required by the Government POC.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

C.5.2.7 SUBTASK 2.7 – Testing Services

The Contractor shall provide the following:

- Test DTS application software, middleware and frameworks using industry standard software quality assurance methods and reporting metrics.
- Maintain, modify or develop test scripts for functional, load, regression, vulnerability and stress testing.
- Execute test scripts, capture test artifacts, record the results and attach all test artifacts in the contractor test management tool.
- Support Government Interoperability test requirements in accordance with Contractors Test Plan.
- Maintain and provide one (1) test environment with external interfacing connections to the PMO for testing. This environment will primarily be used for System Acceptance Testing and any changes made to any financial interfaces that require end-to-end testing. Testing activities will vary in size, scope and duration, requiring the contractor to provide only the baseline environment with interface connections. If additional patches, configuration changes, or data modifications are needed, the Contractor shall be expected to make the changes necessary to execute a successful test event.

C.5.2.8 DELETED.

C.5.2.9 SUBTASK 2.9 – Sustainment/Development Transition to CFE Hosting

The Government desires to transition the DTS application-hosting environment from a GFE system to a CFE ("hosting as a service") system within the next three (3) years, subject to the findings of a cost and feasibility study conducted jointly by the contractor and the government. Upon request of the COR, the Contractor shall provide a Sustainment/Development Transition to CFE Hosting Environment Transition Plan, in accordance with Section F.5.

C.5.2.10 SUBTASK 2.10 – Sustainment/Development Transition-Out Option

The Contractor shall provide a Transition-Out Plan, in accordance with section F.5 to transition application software S/D services to a follow on contractor. It is anticipated that the transition-out would occur at the end of Option Year Four (4) (should all four options be exercised), with a period of performance not to exceed six (6) months to complete final transition.

Four (4) months prior to transition, the Contractor shall submit a detailed transition plan that includes: project schedules, resource estimates, assumptions, and identification of special requirements.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

C.5.2.11 SUBTASK 2.11 – Performance Tuning

The contractor is responsible for tuning logical aspects (i.e., DTS application software, frameworks, middleware and logical configuration items together with the database components) to meet performance requirements.

C.5.2.12 SUBTASK 2.12 – Software Development Life Cycle (SDLC)

The contractor shall have a documented SDLC processes and milestones that will enable creation and delivery of high quality software to the Government. The contractor shall apply these processes in both modifying software for sustainment releases and in developing software for new capabilities for DTS. Modification and development of software must be approved by the PMO in accordance with the approved Configuration Management Plan, which is described in the **Configuration Management** section.

C.5.2.13 DELETED.

C.5.2.14 SUBTASK 2.14 – Software Engineering

The contractor shall carry out software engineering studies and analyses as directed by the COR to create an evolutionary plan for DTS. Objectives of improvements may be in the areas of maintainability, performance, reliability, extensibility, scalability, functionality, usability, or quality of developed code. Studies and analyses may also be required in support of transitioning the hosting environment from a GFE to a CFE ("hosting as a service") environment as discussed in the **Sustainment/Development Transition to CFE Hosting Environment** section.

C.5.2.15 SUBTASK 2.15 – Software Sustainment

The Contractor shall receive DTS application software, data objects and other information assets (as defined in the technical data package) as GFI and shall maintain these as described below. The CDC 2 site serves multiple purposes including use for load, stress and user acceptance testing as well as training. As instructed by the PMO-DTS, the contractor shall provide DTS application software sustainment and maintenance and test all modified software to verify performance in accordance with requirements, and migrate tested and Government-accepted executable software to the hosting environment(s) for installation. The Contractor shall provide sustainment services include:

- Analysis and correction of SPRs.
- Support resolution of TAC ("help desk") trouble tickets received from the DTMO.
- Analysis and correction of application performance degradation.
- Design and implementation of software CRs resulting from Public Law changes or DOD regulatory changes, **accounting system table changes for fiscal year cross-over.**

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

- Full SDLC testing of application software patches and updates.

These services may include maintenance, modifications, updates or additions to existing database tables, data objects and logical frameworks, servers, and middleware products, and configuration support for all such components. The contractor is further required to provide migration support and oversight to the hosting environment for all newly installed application software products and components.

Application software changes will be incorporated into DTS software maintenance releases to provide continual system improvement upon approval of the PMO. The DOD sustainment plan is for an average of four (4) such releases per year.

The contractor is responsible for application software, logical frameworks, middleware and server platforms and tools, data and storage management, and designing and maintaining logical architecture and software data structures (including newly developed capabilities) to be compatible with CDC 1 (production) and CDC 2 (COOP) environments

C.5.2.16 SUBTASK 2.16 – Software Testing and Integration

The contractor shall conduct complete lifecycle testing in accordance with best industry standards and accepted practices. As noted in **Development Services** and **Testing Services** sections, the contractor shall maintain environments for testing of all application software and associated data. These environments shall include the application framework and logical servers to emulate the production architecture together with stub environments to emulate all system-wide interfaces and a database with data objects that are representative of the production environment. The contractor shall provide testing tools to capture all test result artifacts. Prior to conducting any software testing the contractor shall submit the Software Test Description (STD).

The STD describes the test preparations, test cases, and test procedures to be used to perform qualification testing of a CSCI or a software system or subsystem. The STD will be delivered 15 days prior to the Test Readiness Review (TRR) milestone for new development activities. See DoD DID DI-IPSC-81439A for further guidance.

Testing shall include module (white box) and integration (gray box) level testing and remediation, followed by vulnerability, Information Assurance (IA) compliance, regression and functionality testing before delivery to the Government for testing and acceptance. The scope of Government testing will correspond to intended improvements, sustainment corrections and performance enhancements that address the collection of SPR and CR code changes introduced with each Maintenance Release. The Government may perform any combination of integration, functional, regression and qualification test scenarios that support Government acceptance for production fielding of Sustainment and Maintenance Releases Final load and stress testing, along

with user acceptance tests. All testing may be subject to witnessing by the Government designated personnel who will be named prior to the event.

Within ten (10) days of completion of contractor testing the contractor shall deliver the Software Testing Report (STR), all requirements in "IEEE/EIA 12207.1-1997 Lifecycle Data" subsections: 6.29 Test or Validation Results Report. The STR is a record of the qualification testing performed on a CSCI, a software system or subsystem, or other software-related item. See DoD DID DI-IPSC-81440A for further guidance.

C.5.2.17 SUBTASK 2.17 – Software Quality Performance Reports (SQPR)

The contractor shall deliver a software quality evaluation and performance review (SQPR) on the quality of the software in accordance with ISO 9126 and ISO/IEC 12207 for new developed application software within 30 days after software release of new system functionality.

The evaluation of the Software Quality Performance Reports (SQPR) may include manual examination of the code and/or analysis using appropriate software tools, and may be done by a third party entity. This third party will be independent of this contract. However, the Contractor shall be required to meet with the third party entity and may be required to provide the source code and any other pertinent information which enables the third party entity to conduct an independent evaluation of the SQPR's.

C.5.2.18 SUBTASK 2.18 – Configuration Management

The contractor shall maintain a code vault to manage existing and future source and executable software, configurations and configuration management information. The Contractor shall support transition of executable software and configuration artifacts and data objects to the CDC1 and CDC2 hosting environments. The Contractor's code repository shall be compatible with the existing versioning scheme.

The contractor shall prepare, submit, and maintain a Configuration Management Plan (CMP), in accordance with section F.5. The CMP shall apply to all software configuration items and all corresponding software units, and shall conform to the general requirements in the Government CMP. The contractor shall maintain the software units through a version control system, using existing established version designations, in order to maintain baseline integrity within all baselines. The contractor shall also provide traceability of the contractor developed software units to the software configuration items that make up the DTS. The contractor CMP shall also incorporate the change control mechanisms and procedures for managing all change events to include CR, ECP, and fixes to SPRs.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

C.5.2.19 SUBTASK 2.19 – Helpdesk Support

The Contractor shall provide all required Tier 3 (T3HD) helpdesk support. This shall include but is not limited to: resolving advanced problems relating to data or database issues, software defects, interface issues, or other system related problems that range from hardware and networks through software and supporting frameworks.
The Contractor shall directly support all helpdesk activities through in-depth analysis of system components (logical and physical) in a testing environment, develop a get well plan and implement the plan upon approval of the Government. Additional technical support activities may require direct contact with the T1HD and T2HD levels for user assistance support.

C.5.2.20 SUBTASK 2.20 – DMDC Transaction Services (GEX) Support

The Contractor shall provide all required support for the GEX subtask as defined in the task description.

C.5.2.20.1   GEX Integration and Testing Support (Task 1)

The Contractor shall provide all required support the following tasks in conjunction with the PMO-DTS and the Partner Systems.

- Provide logical and physical mappings details on existing data transformation requirements to PMO-DTS and partner system representatives.

- Help partner systems and the PMO-DTS to draft and review change proposals (CPs) that are separate from activities defined in the DTS Task Order.

- Conduct teleconferences for modifications to existing partner system interfaces.

- Conduct unit testing of modified existing physical maps.

C.5.2.20.2   DTS Enterprise Integration Testing (Task 2):

The Contractor shall provide all required support DTS Enterprise testing as it relates to existing partner systems as follows. Support for new systems will have to be evaluated to determine if an ECP is required.

- Maintain the GEX test platform with 80% uptime including test connection configuration/verification for DTS test events. This includes support to existing partner system interface test activities with Government provided test data and test scenarios.

- Generate user accounts and support security protocols for the test platform.

- Troubleshoot connectivity issues with all partner systems including DTS.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

- Conduct point-to-point (P2P) testing including scenario and test data for existing partner systems.

- Support the system qualification testing (SQT) conducted by the PMO-DTS.

- Correct mapping bugs identified during the SQT. Deficiencies or changes in requirements will be evaluated by ECP.

- Participate in daily PMO-DTS test meetings such as hot washes and Test Review Board (TRB).

- Provide copies of test data when requested to support troubleshooting.

C.5.2.20.3   Production Deployment and Support (Task 3):

The Contractor shall provide all required production support as follows:

- Troubleshoot production connectivity issues.

- Coordinate changes for IP addresses, username/password changes – ongoing production support.

- Support for release upgrades, partner system software/middleware changes of existing interfaces that may result in connectivity or map configuration changes.

- Coordinate the restage of data when an issue arises that prevented the data from being posted by a partner system successfully including DTS.

- Research of translation issues or failures which may result in map changes.

- Support discussions and coordination of system migrations from one database to another.

- Maintain the interface deployment guides (IDG) to support production configurations at DMDC Transaction Services GEX.

- Generation, testing and delivery of production map updates and shared libraries (when necessary) to DMDC Transaction Services GEX.

C.5.2.20.4   DMDC Migration Support (Task 4):

The Contractor shall work with DMDC Transaction Services to coordinate the migration tasks for the DTS partner system connections from the GEX at DECC Ogden to the GEX at DMDC Transaction Services. These tasks include:

- Coordination of approach for transition to DMDC Dayton including input to a migration schedule as derived by DMDC Transaction Services.

- Provide documentation of existing partner system configurations in formats required by DMDC Transaction Services.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

- Provide training support to DMDC Transaction Services on DTS-GEX transaction flows and data types.

C.5.2.20.5   Analysis Support (Task 5):

The Contractor shall work collaboratively with the PMO-DTS to provide contract support as follows:

- Provide Engineer Change Proposals (ECPs) in response to Functional Requirements Documents (FRD) and Change Proposals (CPs), or equivalent, for enhanced, modified or new software capabilities.

- Project meeting participation such as technical and status meetings as requested by the PMO-DTS.

- Support FISCAM audit working group questions and requests for Northrop Grumman generated documentation.

C.5.3 TASK 3 – BUSINESS INTELLIGENCE AND REPORTING SERVICES

The contractor shall support the Data Mart and the Business Intelligence (BI) tool as required. This includes but is not limited to maintaining and developing the database, data objects and BI tool objects as defined below

C.5.3.1 SUBTASK 3.1 – Recurring and Ad Hoc Reports

The contractor shall support all requests for recurring and ad hoc and monthly reports. These reports will be pulled from the existing database data and/or the archive database data. The Contractor shall be provided a list of all monthly reports that are re-occurring, but may have additional reports due on a case by case basis. Monthly data pulls shall take three (3) working days (or less) to complete. Larger data pulls may take longer but the contractor is required to provide a delivery date within twenty-four (24) hours after receiving the request The contractor shall also provide Ad Hoc reports. These reports could include but not be limited to investigative inquiries; Freedom of Information Act (FOIA) requests; Inspector General (IG), Government Accountability Office (GAO), supporting criminal investigations and other Government Agencies that request data for their agencies. These data pulls shall not take longer than five (5) working days complete. When more involved requests are anticipated to take longer, the contractor is required to provide a delivery date within twenty-four (24) hours which will be subject to Government approval in cases where it exceeds the five (5) working day requirement. In case of national and/or weather emergencies, the Contractor shall be required to pull the data within hours of receiving the request. Typical data that is required for these types of requests are a list of personnel within a set location area.

The list of current reports is in Section J, Attachment J (Recurring Report List).

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

C.5.3.2 SUBTASK 3.2 – Compliance Auditing

The contractor shall be required to support external auditing efforts relative to determining the system's compliance with federal laws, regulations and policies, including but not limited to: A123, Federal Information Systems Control Audit Manual (FISCAM), DIACAP, Federal Financial Management Improvement Act (FFMIA), Statement on Standards for Attestation Engagements, No.16 (SSAE-16) and related regulatory requirements. In addition to supporting the resolution of preliminary audit findings, the contractor shall be required to work with external audit personnel to provide access, information, and demonstrate compliance with controls mandated for system compliance. Information is needed in real-time or near real-time about system areas, which may have potential vulnerabilities/violations. Final audit reports are expected to include documenting non-conformances and corrective actions associated with assessments/inspections. The contractor shall be required to develop remediation plans which include a method to manage resulting actions to include identifying and tracking and verification of actions taken. The contractor shall deliver a Compliance Auditing Support Plan, in accordance with Section F.5, to address any unresolved preliminary findings at time of award, their plan for supporting future audits, and their standard practice for supporting audit compliance and reporting and remediation of actionable items.

C.5.3.3 SUBTASK 3.3 – Business Intelligence Development and Support

DTS reporting is available to DTS users worldwide through a COGNOS^R reporting tool that is part of DTS. The contractor shall operate and maintain this COGNOS^R reporting tool and its associated data mart. This tool is installed in the DTS production environment. The contractor shall use the existing ETL tool to populate and maintain a data mart that is optimized for this COGNOS^R reporting. The contractor shall operate this reporting tool and data mart such that data reported will be no more than twenty-four (24) hours behind the production's transactional data. The contractor may see spikes in reporting requirements due to auditing and travel compliance needs. The contractor shall optimize the reporting tool and associated data mart such that these spikes do not impact the above reporting requirements.

In addition, the contractor shall develop all reoccurring reports in the data mart. The contractor shall remove the reoccurring reports from the current DTS Reports Scheduler reporting tool as they are developed in the data mart with the goal of eliminating the Reports Scheduler tool from DTS.

C.5.4 TASK 4 – INFORMATION ASSURANCE (IA)/SECURITY/IT CONTINGENCY PLAN

In the conduct of the limited "First Traveler" Pilot testing under CLIN 2004, the contractor will not be held responsible for the requirements in this section (C.5.4 Task 4).

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

The Contractor shall perform IA on DTS Hosting system. IA covers all actions that protect and defend the DTS information system by ensuring availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of the DTS information system by incorporating protection, detection and reaction capabilities.

The Contractor shall coordinate and support Certification and Accreditation (C&A) process when periodic re-accreditation is required or as a significant system change dictates the need with the COR. DTS is a Mission Assurance Category II, Sensitive (MAC II) system and its IA posture is maintained by implementation of IA Controls of DODI 8500.2, E4, along with any DMDC required controls and requirements.

Contractor shall maintain DTS System Accreditation by continuously monitoring DTS IA posture, and through reviewing IA control implementation and revalidation of those controls as dictated by significant system changes. The Contractor shall perform Phase Four DIACAP tasks along with DMDC requirements consistent with maintaining DTS Accreditation such as:

- Incorporating any new or modified IA Controls
- Mitigating any identified security vulnerabilities
- Conducting monthly vulnerability scans utilizing DISA Field Security Office (FSO) approved methods and standards
- Supporting Government directed penetration testing no less than every two (2) years or after a major security breach.
- Executing DTS Plan of Action and Milestones (POA&M) actions maintained by DTS Enterprise Mission Assistance Support Service (eMASS) and VMS

The Contractor shall comply with the following security requirements:

- Contractor shall provide a copy of all IA security scans to DMDC Computer Network Defense Service Provider (CNDSP) and the IAM, and shall upload scan results to the DTS Vulnerability Management System (VMS) within prescribed timelines of the DTS VM Plan.
- Contractor shall provide a copy of security logs and remote user access logs to the DMDC CNDSP and the IAM in accordance with existing DMDC policy on a monthly basis.
- Contractor shall continue implementation and maintenance of Host Based Security System (HBSS) on all DTS servers, providing monthly metric updates to the DMDC CNDSP and the IAM to monitor compliance.
- Contractor shall update DMDC/DTS eMASS application by providing updates and artifacts related to IA controls for approval by the Government representative and the IAM as instructed by the PMO.
- The contractor shall provide yearly (at a minimum) most current DIACAP and component IA control artifacts in accordance with DODI 8510.01.
- Contractor shall populate/maintain DMDC/DTS VMS and provide mitigation strategies

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

for Government and DMDC CNDSP review and approval related to open items. Contractor shall provide listings of CAT 1 and 2 items that require POAM or Risk Assessment approval using POAM template provided by DOD IAM. The template requires explanation detailing when each finding will be closed, or why a finding cannot be closed if a Risk Assessment is needed.

- Contractor shall comply with security investigations for privileged users as stated in DODI 8500.2, E3.4.8 DoDI and in accordance with guidance provided by DOD.
- Contractor shall comply with United States Cyber Command (USCYBERCOM) orders and directives, and implement changes to DTS as required by USCYBERCOM.
- Contractor shall ensure that all software and hardware are covered under maintenance and support agreements with specific vendors in accordance contract requirement. Items not covered under an agreement, or no longer supported by maintenance agreements, shall be reported to the Government monthly per DODI 8500.2. Hardware and software shall be maintained and configured per DOD Security Technical Implementation Guide (STIG) and Information Assurance Vulnerability Alerts (IAVA), to include IAVA patches.
- Deleted.
- The Contractor shall provide a IT Contingency Plan in accordance with Section F.5.
- The contractor shall use NIST SP 800-34, Rev 1, Contingency Planning Guide for Information Technology Systems to develop the IT Contingency plan and format.
- Contractor shall participate in an annual COOP and Incident Response exercise developed by the PMO-DTS and providing information to the PMO-DTS for their completion of after action reports.Deleted.
- Contractor shall comply with requirements of the Office of Management and Budget (OMB) Memo 06-16, Protection of Sensitive Agency Information, DOD Memorandum of June 23, 2006 and DOD Guidance on Protecting Personally Identifiable Information (PII), and DMDC Policy and Procedures when Personal Information is Lost, Stolen or Compromised.
- Contractor shall notify the DTS IAM within one (1) hour in the event of a PII Incident.
- Contractor shall provide information regarding the PII incident to assist the PMO-DTS investigation of the PII incident.
- Contractor shall comply with technical certification and training as specified in Department of Defense Instruction (DODI) 8570.01-M Information Assurance Workforce Improvement Plan, through Change 3, of April 2010 through life of the contract.
- The software shall not contain any code that does not support a software requirement.
- The Contractor-developed software shall be free from all computer viruses, worms, time-outs, time bombs, back doors, disabling devices and other harmful or malicious code intended to or which may damage, disrupt, inconvenience or permit access to the Software user's or another's software, hardware, networks, data or information.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

The Contractor shall maintain DTS Security in accordance with current DODI 8500.2 IA Implementation, DODI 8510.0 I DIACAP and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 NIST 800-53_rev4 requirements.

C.5.4.1 SUBTASK 4.1 – Disaster Recovery, COOP, and Contingency Planning

Contractor's location for the CDC 2 backup/COOP site must provide adequate geographic separation from CDC 1 to ensure disaster survivability, while also ensuring the physical separation of the sites does not jeopardize the requirement for 0% data loss during a system fail-over. The fail-over time from CDC 1 to CDC2 shall not exceed 24 hours. The Contractor's proposal shall include a risk analysis assessing the vulnerability of the CDC 2 site to the same disaster event as one anticipated to occur at the CDC 1 site (e.g., seismic, weather-related, terror attack or power grid failures etc.) and also describe the technical approach for ensuring 0% Approved Transactional data loss upon fail-over.

The Government will schedule one (1) annual exercise or assessment where fail-over to the COOP site is demonstrated. The Contractor shall support the IT Contingency Planning efforts and exercises as required and is responsible for communications, networks, system administration, and hardware/software (operating systems and other commercial software) support including all the DTS software.

Data loss is defined as any transactional information or session information that is inserted in or committed to the database in CDC1.

C.5.5   TASK 5 – PROVIDE PROGRAM MANAGEMENT (CLIN X001)

The contractor shall provide program management support under this TO from Task Order award and project kick-off through transition-out. This program management shall include status reporting, status meetings, Project Management Plan, trip reports, Quality Control Plan, and Earned Value Management.

This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Statement of Work (SOW). The contractor shall identify a Program Manager (PM) by name who shall provide management, direction, administration, quality control, and leadership of the execution of this TO. The contractor shall schedule meetings and provide deliverables in accordance with Section F.

C.5.5.1   SUBTASK 5.1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule and coordinate a Project Kick-Off Meeting at the location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include vital

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

contractor personnel, representatives from the directorates, other relevant Government personnel, and the FEDSIM COR. The contractor shall provide the following at the Kick-Off meeting:

1. Updated Transition In Plan
2. Project Management Plan
3. Final Quality Control Plan (QCP)
4. Earned Value Management (EVM) Plan.

C.5.5.2 SUBTASK 5.2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor PM shall develop and provide an MSR (Section J, Attachment B) using Microsoft (MS) Office Suite applications, by the tenth calendar day of each month via electronic mail to the DMDC Technical Point of Contact (TPOC) and the COR. The MSR shall include the following:

1. Activities during reporting period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
2. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
3. Personnel gains, losses, and status (security clearance, etc.).
4. Government actions required.
5. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
6. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for the reporting period).
7. EVM statistics.
8. Accumulated invoiced cost for each CLIN up to the previous month.
9. Projected cost of each CLIN for the current and next month.
10. Update/s of each software release (include SPRs) and provide the contents of the release.

C.5.5.3 SUBTASK 5.3 – CONVENE TECHNICAL STATUS MEETINGS

The contractor PM shall ensure attendance of all appropriate personnel (key personnel, functional leads, contracts, and other mutually agreed upon attendees) at the bi-weekly, Integrated Staff Meeting. The purpose of this meeting is to ensure all stakeholders are informed of the upcoming (short and long-term) activities, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities.

C.5.5.4 SUBTASK 5.4 – PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The PMP shall:

1. Describe the proposed management approach
2. Contain a definition of all tasks
3. Include milestones, tasks, and subtasks required in this TO

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

4. Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between or among Government organizations
5. Include the contractor's QCP and EVM Plan.

C.5.5.5   SUBTASK 5.5 – UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP is an evolutionary document that shall be updated annually at a minimum. The contractor shall work from the latest Government-approved version of the PMP.

C.5.5.6   SUBTASK 5.6 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted. The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, purpose, duration of trip, and point of contact (POC) at travel location.

C.5.5.7   SUBTASK 5.7 – UPDATE QUALITY CONTROL PLAN (QCP)

The contractor shall update the QCP submitted with their proposal and provide a final QCP as required in Section F. The contractor shall periodically update the QCP, as required in Section F, as changes in program processes are identified.

C.5.5.8   SUBTASK 5.8 - EARNED VALUE MANAGEMENT (EVM)

The contractor shall employ and report on EVM in the management of this TO. See H.19, Earned Value Management, for the EVM requirements. This will only apply to the development CLIN x004.

C.5.5.9   SUBTASK 5.9 - INTEGRATED MASTER SCHEDULE (IMS)

The Contractor shall ensure there is a time phased planning tool that uses a calendar or detailed schedule to demonstrate how work efforts will support tasks and events. The IMS is required to integrate with the existing DTS Master Schedule.

C.5.5.10   SUBTASK 5.10 - RISK MANAGEMENT PLAN (RMP)

The Contractor shall document all plans and actions taken to identify, assess, mitigate, and continuously track, control, and document program risks, which is tailored to DTS requirements.

C.5.5.11   SUBTASK 5.11 - REQUIREMENTS TRACEABILITY MATRIX (RTM)

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056

The Contractor shall update and maintain a Requirements Traceability Matrix (RTM), in accordance with Section F.5, to list all system/component requirements, and detail how and where they are addressed in the system design. The Contractor shall work with the PMO-DTS to determine the form/format of the RTM, tools to be used, etc.

C.5.5.12 TRANSITION-OUT

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The Contractor shall provide and implement a Transition-Out Plan in accordance with Section F.5. The Contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

- Project management processes
- Points of contact
- Location of technical and project management documentation
- Status of ongoing technical initiatives
- Appropriate Contractor-to-contractor coordination to ensure a seamless transition
- Transition of Key Personnel
- Schedules and milestones
- Actions required of the Government

The Contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

Task Order GST0013AJ0081
Modification PO36
Contract#GS00Q09BGD0056